1. A method of cryptographic encryption, comprising the steps of:

a) selecting, by a recipient, a modulus p from a group of equations consisting of:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where $r /= 1$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where $r /=1$, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r;$$

b) selecting, by the recipient, a curve E and an order q;

c) selecting, by the recipient, a base point $G=(G_x,G_y)$ on the elliptic curve E;

d) generating, by the recipient, a private integer w;

e) generating, by the recipient, a public key W, where W=wG;

f) distributing, by the recipient, p, E, q, G, and W in an authentic manner;

g) retrieving, by a sender, the recipient's public key W;

h) generating, by the sender, a private integer r;

i) generating, by the sender, $R=rG$ using the form of recipient's modulus p, and where G is recipient's basepoint;

j) combining, by the sender, r, W, and M using the form of the recipient's modulus p to form ciphertext C; and

k) sending, by the sender, (R,C) to the recipient.

2. The method of claim 1, further including the steps of:

a) retrieving, by the recipient, the recipient's private key w;

b) receiving, by the recipient, (R,C) from the sender; and

c) combining, by the recipient, R, w, and C using the form of the recipient's modulus p to recover M.